Microsoft Corporation Response to Federal Identity Theft Task Force Request for Comments January 19, 2007

Identity Theft
Task Force, P065410

Filed Electronically to:
taskforcecomments@idtheft.gov

Microsoft Contacts:
Jeffrey Friedberg – jeffreyf@microsoft.com
Frank Torres – ftorres@microsoft.com

Microsoft is pleased to submit the following response to the request for comments by the President's ID Theft Task Force. We look forward to continued collaboration between the Task Force, federal agencies, the private sector and other interested parties in finding solutions to preventing and addressing ID theft. Microsoft appreciates the opportunity to provide comments and any future opportunities to contribute to this important effort.

I. MAINTAINING SECURITY OF CONSUMER DATA

1. What steps could help reduce reliance on SSN by local, state, and federal agencies?

A key step is to find an alternative way to identify people - one that supports "Federated Identity" and ensures strong mutual authentication. In the online world, it is important not to be locked into any one particular technology. Creating an "Identity Metasystem" that is built on open standards would reduce risks, lower costs, and allow a wide variety of existing and future solutions to be leveraged. Another critical component is establishing a better user experience for exchanging Identity information and authenticating individuals. It would be easy for people to use and would not rely solely on shared secrets like username and passwords which are often forgotten and compromised.

2. Would minimizing the use of SSN in private sector help address ID theft?

Yes, to the extent obtaining an SSN allows a criminal to commit identity theft minimizing SSN use could potentially lower the opportunity for ID theft.

Unfortunately, limiting SSN use would not make the general problem of ID theft go away. When a SSN is stolen, many relationships are at risk. If multiple alternative ID's are used instead, then the impact of a breach could be reduced (in the limit, one ID per relationship would limit the damage of a breach to just that relationship). Using multiple IDs to identify a person means the bad guy has to work harder (more IDs to steal). Note, the alternative IDs could still be stolen by the bad guy if authentication remains weak and one way. Rather than just create alternative IDs, a more secure mechanism should be deployed – e.g. one that does not rely on sharing secrets. Public Key Cryptography is such a mechanism.

3. **Would imposing National Data Security Standards on commercial entities that maintain sensitive consumer information help address deficiencies in current practices? What would they look like? Does the need vary by business sector, model, or size? What would the costs be on business?**

   Yes, standards could help. They would help ensure only the data that is required for the business purpose is collected, that secure methods are use during transport and storage, that only those with a need to know have access, that data is retained only as necessary, and that consumers could inspect the data and correct it to insure its integrity. The need for such a standard is mostly driven by the type of data being processed versus business sector, model, or size. Obligations already exist for businesses to properly protect such data (e.g., GLBA and HIPPA) so following these types of rules should not add additional costs (unless formal certification and/or regular audits are also required). The Task Force should consider reaching out to interested parties to more fully understand actions currently being taken to protect data.

4. **Would imposing a National Breach Notice Requirement on commercial entities that maintain sensitive consumer information help address deficiencies in current practices? What would they look like? Does the need vary by business sector, model, or size?**

   Yes, standards could help. They would help ensure a consistent bar for when notices should be sent, what they should contain, and whom they should be sent to. However, setting such a standard is challenging in that the content of the notice depends on the context of the breach (e.g. encrypted data is less likely abused) and the context can vary widely (e.g. data is lost versus stolen). The need for such a standard rises with the size of the database a business maintains. As the numbers go up, the likelihood a person will get multiple notices from different businesses goes up as well; therefore, receiving a consistent set of notices could help the person better assess the risks they are under and take appropriate action. That said, having a standard might also help smaller businesses craft their notices since they have the same obligation to let their customers know, but perhaps have fewer resources to craft such a notice and could benefit from a well thought out template.

5. **Are campaigns to educate the private sector an appropriate way to address identity theft? What are the essential elements?**

   Education is an important element in addressing ID theft, especially where social engineering techniques are used by criminals to trick consumers into revealing information that could compromise their identity, allow access to bank accounts, or otherwise result in ID theft. Educational campaigns, however, are just one tool in a comprehensive strategy to address identity theft. Technology investments, industry cooperation, stronger enforcement, and legislation as needed are complementary efforts that are also required. For consumers, the essential elements of such a campaign include helping them recognize fraudulent activity before they turn over their secrets to a bad guy and what to do if they think they have become a victim. For businesses, it's helping them understand what steps they should take to provide strong mutual authentication to their customers, how to be a responsible data custodian, and how to properly react when a breach occurs to minimize the scope and harm.

II. PREVENTING THE MISUSE OF CONSUMER DATA

1. **Beyond holding workshops on improving authentication, are there other measures that should be considered?**

   While we wait for improved authentication (e.g. the deployment of PKI based systems), investigate ways to make existing systems more robust (those that still rely on shared secrets like username and password). Also, need to make sure critical infrastructure, such as Certificate Authorities (CAs) are hardened to reduce the chance of abuse (e.g. via Extended Verification Certificates).

III. VICTIM RECOVERY

1. **Would training LE, first responders, counselors help them provide better assistance to victims? Would creating a statement of rights help victims? Are there other ways to help?**

   Yes, with appropriate collateral, these steps could assist victims. Additional ways to help include making it easier to report ID theft, recover losses, and stop subsequent abuse. The latter talks to the need to more easily revoke and reissue a SSN if it has been compromised. This is another area where a stakeholder discussion may be helpful to identify what are current best practices, as well as explore additional areas of victim assistance that should be considered.

2. **In addition to allowing a victim to seek restitution for their lost time, what other obstacles could be removed for recovery?**

   As stated above, helping victims revoke and reissue compromised credentials. Another area to investigate is making it easier for victims to control the issuance of new credit in their name. One approach is to work with the various industry *sectors to develop and implement a more robust system that allows credit agencies and lenders to better authenticate the person requesting credit (e.g. perhaps by implementing a system that enables a person to authenticate with a private key that matches a public key the consumer originally posted in their credit report).*

3. **Would having a nationwide system that helps a victim not be mistaken for the criminal be helpful? If so, what are the essential elements?**

   Yes, having a voluntary system that helps victims distinguish themselves from the criminals that pretend to be them (e.g. via an ID theft victim "passport") could be essential recovery tool. The credentials issued should not expose the victim to similar exploits that made them a victim. More secure methods should be used (e.g. a physical smart card that uses PKI).

4. **Are studies that assess the effectiveness of amendments and related laws important for formulating a national strategy to combat ID theft? Are there other studies that should be done?**

   Rather than focus on specific amendments and laws, what would be helpful is to come up with a common way to measure ID theft. There are many aspects to this problem and the numbers that are reported vary widely. The proof that any investment was worth it rests on our ability to measure whether it was effective. Without common nomenclature and a methodology for measurement, we cannot track our progress or identify which specific issues deserve our attention over others that have less impact. We also believe that bringing together all of the key stakeholders to be part of developing a national strategy on ID theft will be an important element to any successful effort.

IV. LAW ENFORCEMENT: PROSECUTING AND PUNSIHING IDENTITY THIEVES

1. **Would establishing a national center for law enforcement help them respond to ID theft? What would be its core functions?**

   Yes, it could help them respond to ID theft. As we have learned, the bad guys are using a strategy called "spread the pain" where they commit crimes across multiple jurisdictions just under the threshold for local law enforcement to take action. Having a center could help law enforcement "aggregate" the crimes and spot larger targets worthy of their attention. The challenge is collecting enough data to identify patterns and to do so in a way that protects the privacy of the victims. This mission could be assigned to an existing organization such as the Internet Crime Complaint Center (www.ic3.gov), and if a new center is created, it should be aligned with existing organizations to minimize duplication and increase capability.

2. **Would improving the ability of law enforcement to access documents, increasing dialogue with financial services industry, and making it harder to obtain credit from a victim, meaningfully assist law enforcement?**

   As stated above, increasing access to relevant materials while protecting a victim's privacy could help law enforcement spot criminals. Collaborating with financial institutions could help both parties better understand the issues and test the efficacy of solutions. Ensuring credit is issued to the right person, as many financial systems do today, helps keep a key problem (new account fraud) from getting bigger.

3. **Would encouraging foreign countries to make ID theft illegal, accept the Convention on Cybercrime, and eliminate safe havens help our law enforcement pursue foreign based ID thieves operating in the United States? Should we assist, train, and/or support foreign law enforcement with their cases? Should we enhance our ability to provide rapid international cooperation?**

   There is no way around it. ID theft is a world-wide problem and we cannot address the entire problem from our shores. World-wide collaboration is necessary. The suggestions above could positively impact the efficacy of that effort (any specific legislative changes would need to be discussed in more detail). In particular, the US should continue its efforts to provide universal accession to the Convention on Cybercrime. That said we need to be careful when sharing confidential information of victims. Privacy laws and constitutional protections vary and we need to maintain a high bar to ensure sensitive data is protected.

4. **Would having a coordinator for each United States attorney's office and creating working groups that focus on investigations help increase the number of ID theft prosecutions?**

   These steps might help, however, the virtual distributed nature of online fraud makes it especially hard to identify and bring to justice those that are responsible. Better tools to detect and track down the criminals are also required, along with better international cooperation. Also of importance is ensuring penalties and recommended sentences are of sufficient magnitude, including at the federal level, to interest investigators and prosecutors as well as deterring criminal conduct.

5. **Would special enforcement activities focused on SSN sales, health care related ID theft, or ID theft by illegal aliens help in prosecution? What other activities could help?**

   While these efforts could help, the bigger question is knowing whether or not this is the best place to put our resources. As stated earlier, having accurate statistics for how and where the most damaging ID theft is happening is essential for making such tradeoffs. For example, are ID thieves rampant among *undocumented aliens here in the US or are most based in a foreign country (e.g. eastern Europe)? If so, it would be a better use of resources to pursue the latter.*

6. **Would amending statues assist prosecutors in charging, convicting, and punishing ID thieves?**

   Certain changes would be helpful. Eliminating the requirement for an interstate communication where it is not necessary for constitutional purposes, such as in 18 U.S.C. § 1030(a)(2)(C), would broaden federal jurisdiction. However, the requirement of "damage" should not be removed from § 1030(a)(5) because that section is specifically about causing "damage," and, for example, removing "damage" from (a)(5)(A) would make transmission of any code a crime. However, removing the $5000 damage jurisdictional threshold for criminal prosecutions does make sense if other requirements are met (it is important not to impose undue burdens on the federal courts), for example, ten or more computers are affected. This could accomplished by adding a new § 1030(a)(5)(B)(vi) which would permit criminal prosecution when conduct causes damage affecting ten or more computers in a one-year period. It is also of critical importance to ensure that the Sentencing Guidelines recommend appropriate sentences for identity theft.

   Any statutory changes need to be discussed in detail, of course, to avoid unintended consequences. Penalties for misuse of customer data need to be appropriate to the conduct; for example, it seems extreme to suggest that a company employee who knowingly transfers a customer's data without authorization, but believing in good faith that an exception exists, has committed a federal felony.

   With the recent passage of a new law addressing pretexting, some of the issues raised in this question may have been addressed.

7. **Would enhancing ID theft training help law enforcement and prosecutors?**

   Those that need to address this dynamic evolving issue require comprehensive up-to-date training and associated collateral. In addition to the public sector sources listed, other private sector communities could be leveraged (both industry and academia).

8. **Would surveys related to law enforcement activities be helpful? What other surveys should be considered?**

   Yes, tracking such activities can be one part of a scorecard that lets us see whether our mitigations are having the desired effect. Other surveys that would help are those that give us a better view on the problem space so we can track which methods of ID theft are growing / shrinking and how big / small are the losses.